DAY 8: Can Bitcoin be Hacked?

1 message

21 Days of Bitcoin <education@bitcoinmagazine.com>
Reply-To: 21 Days of Bitcoin <education@bitcoinmagazine.com>
To: samglaj3p@gmail.com

Wed, Aug 24, 2022 at 10:41 PM

You might have heard the alarming stories of DeFi and cryptocurrency exchange hacks...

Need a reminder? Bitcoin exchange Mt. Gox was famously hacked in 2014 and $460 million worth of bitcoin — equivalent to $38 billion today — was stolen. Ouch.

Just recently, a hacker stole $600 million worth of various cryptocurrency assets from DeFi project Poly Network. Most of the funds have since been returned, but I can't imagine putting your trust and securities into an exchange, just to have a shadowy super coder make away with all of your investments.

With the cryptocurrency industry being hacked left and right, it's important to proceed with caution. However, there are ways to protect

yourself from these hacks: take your bitcoin off exchanges, and don't play with altcoins.

In a few days, I'll walk you through buying, transacting, and self-custodying bitcoin, step by step. But today, I want to discuss cryptocurrency network hacks. Specifically, why bitcoin is specially "unhackable" compared to the other cryptocurrency networks (DeFi/altcoin projects). While it's technically possible for the Bitcoin network to be hacked and funds to be stolen directly off of the blockchain, it will never happen with bitcoin (though, it can and does happen to other cryptos).

Here's why.

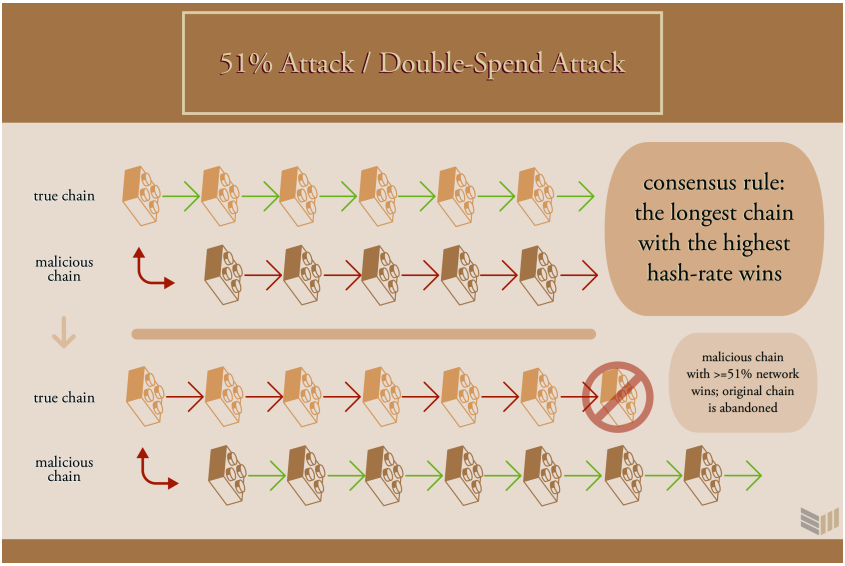
The 51% Attack

The reason why the Bitcoin network is so strongly decentralized is because of how many participants there are in it. With each additional

miner and node that comes online, the overall security of the network is strengthened, and it becomes increasingly harder for some malicious entity or group to try and take over the network.

But if a blockchain network is not strong, then it is prone to something called a 51% attack, where if miners are able to gain a hold of over 50% of the network, they can effectively take over and "double spend" their existing crypto. Similar to counterfeit bills, hackers would be able to use "fake copies" of an existing cryptocurrency, thus inflating the supply and devaluing the currency.

A 51% attack on proof of work protocols like bitcoin are able to take place successfully since the network will always default to the longest chain with the highest mining power as the chain of truth.



But ultimately, this won't happen on the Bitcoin network because Bitcoin's proof of work algorithm requires a lot of power for a 51% attack to occur (as much power as a small country consumes along with more than $23 billion worth of hardware alone); it wouldn't make much sense for a hacker to spend this much money in an attempt to make risky money.

Additionally, hackers cannot "steal" bitcoin from others — they can only "double-spend" their own bitcoin, just as counterfeiters make fake dollar bills instead of robbing a bank. Once again, this would be foolish to do because the value of bitcoin would quickly drop as the network recognizes that bitcoin has been double-spent and people start to lose confidence in bitcoin.

Quantum Computing Concerns

Many skeptics also bring up the concern for quantum computing rendering the Bitcoin network's security useless, since quantum computing would be able to break the network's encryption algorithms and reveal users' private keys.

Another concern is that quantum computing could allow for "super miners" that can mine bitcoin at an extremely high speed, thus centralizing mining and allowing them to take control over the chain.

While these situations may appear daunting, they are far off into the future of quantum computing. In any case, the Bitcoin network has much time to "upgrade" to prepare for such dire circumstances and will inevitably be able to protect itself from any sort of attack we see coming. To do this, Bitcoin would "hard fork" to a protocol that accommodates quantum-secure features (tomorrow I'll go over what it means for a cryptocurrency to "fork").

What Can You Do To Protect Your Bitcoin?

For now, just continue to execute your best internet security practices, such as using password generators and turning on two-factor authentication for your crypto exchange accounts. Later on, I'll teach

you how to transfer your bitcoin off of exchanges and into your own self-custody solutions to prevent your bitcoin from potential hacker theft.

However, a word of warning: self-custody isn't an inherently simple task yet for most people. It's imperative for the industry to continue to develop and optimize user-experience for bitcoin wallets, but also to hold exchanges accountable for safeguarding people's funds who aren't ready for self-custody storage solutions yet. Ultimately, self-sovereignty is the end-goal for securing your bitcoin — but remember to take the time to learn first.

The nuances of bitcoin security go layers deep — if you have any questions, feel free to tweet them using the hashtag **#21DaysofBitcoin**.

Hats, shirts, mugs + more

Take 21% off our collection of bitcoin shirts, hats, or mugs from the official Bitcoin Magazine store.
Promo code: **"STORE21D"**

Bitcoin Magazine Print

Take $12 off your annual print subscription. Get 4 issues/year to your mailbox, starting with The Censorship Resistant

Issue.
Promo code: **"21DAYS"**

Bitcoin Magazine PRO

Save 40% off your first year subscription with Bitcoin Magazine PRO. Insights on bitcoin markets, global macro, & in-depth research reports published monthly.
Take 40% off